



Perceptions about Self-Encrypting Drives

A Webcast on the Survey Results

Sponsored by the Trusted Computing Group

Independently conducted by Ponemon Institute
May 10, 2011 1:00pm EDT/10:00am PDT

Webcast Logistics

No Sound?

- Make sure that you have dialed in correctly:
 - Toll free: 1-888-909-7654
 - Participant Passcode: 314675
- Press *0 to reach an operator if you are still experiencing difficulties

Questions?

- If you have questions throughout the duration of the presentation:
 - Select the question mark icon on the top navigation
 - Type your question
 - Watch/listen for a response

This webcast will be archived and accessible at:
http://www.trustedcomputinggroup.org/media_room/events/99

Today's Speakers

- **Brian Berger**, TCG Director, Executive Vice President Marketing & Sales, *Wave Systems Corp.*
- **Dr. Larry Ponemon**, Chairman and Founder, *Ponemon Institute*
- Technical Experts from the Trusted Computing Group
 - **Darren Lasko**, Principal Storage Security Architect, Storage Technologies Group, *Intel*
 - **Dr. Michael Willett**, Storage Security Strategist, *Samsung*

Perceptions about Self-Encrypting Drives: A Study of IT Practitioners

Sponsored by the Trusted Computing Group

Independently conducted by Ponemon Institute

May 10, 2011

Ponemon Institute LLC

- ✓ The Institute is dedicated to advancing responsible information management practices that positively affect privacy and data protection in business and government.
- ✓ The Institute conducts independent research, educates leaders from the private and public sectors and verifies the privacy and data protection practices of organizations.
- ✓ Ponemon Institute is a full member of **CASRO** (Council of American Survey Research Organizations). Dr. Ponemon serves as CASRO's chairman of Government & Public Affairs Committee of the Board.
- ✓ The Institute has assembled more than 60 leading multinational corporations called the **RIM Council**, which focuses on the development and execution of ethical principles for the collection and use of personal data about people and households.
- ✓ The majority of active participants are privacy or information security leaders.

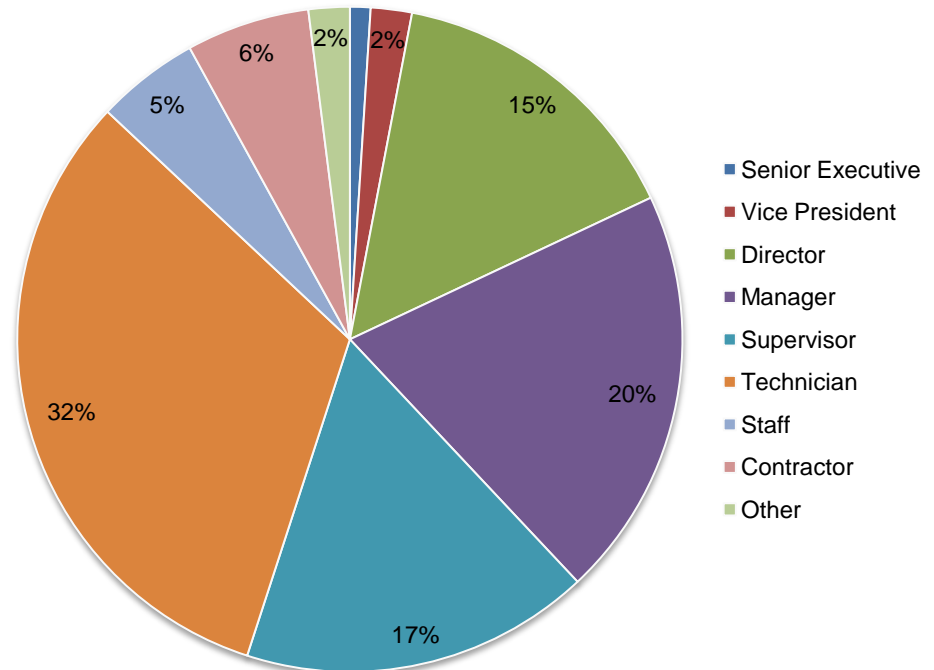
About our study

- We conducted the first national national survey to determine IT security practitioners' views about hardware-enabled security technologies and, more specifically, self-encrypting drives.
- Sponsored by the Trusted Computing Group (TCG) our study utilized a representative sample of IT and IT security professionals. Sampling and screening procedures will ensure that respondents are presently in the workforce in the United States and have bona fide credentials.
- To accomplish this study, we will work closely with TCG to create and develop a mutually acceptable survey instrument. By design, this final instrument utilized a series of 20 fixed format questions.
- The primary collection channel was a secure extranet Web site. No personally identifiable information was collected from the respondent. In addition, all survey results will be conducted in conformance with CASRO ethics and privacy practices.

About our sample

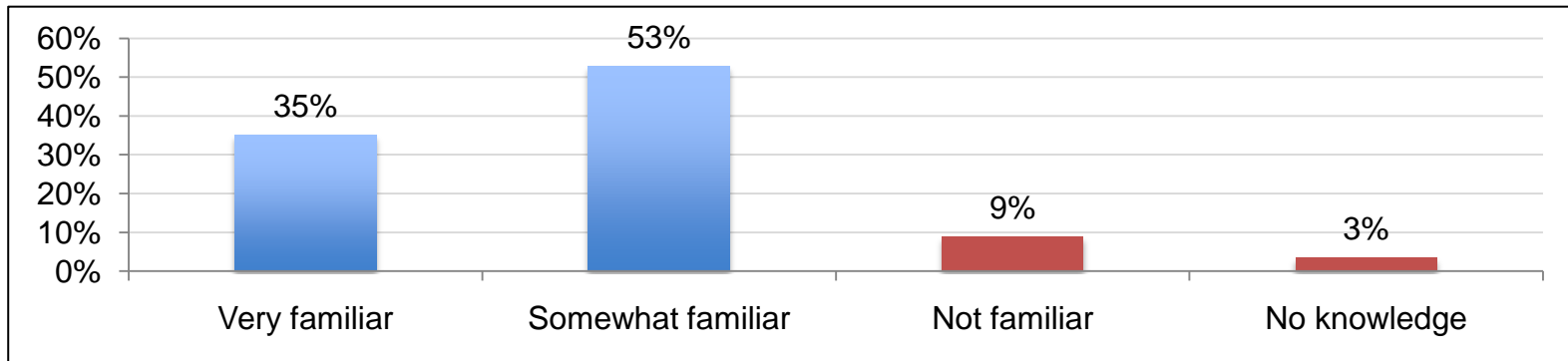
A sampling frame of more than 15,700 IT and IT security practitioners located in US organizations was used to obtain 655 completed surveys. After applying screening criteria, the final sample consisted of 517 respondents with bona fide credentials.

Sample response	Freq	Pct%
Total sampling frame	15,749	100.0%
Total survey returns	719	4.6%
Rejected surveys	64	0.4%
Sample before screening	655	4.2%
Final sample	517	3.3%

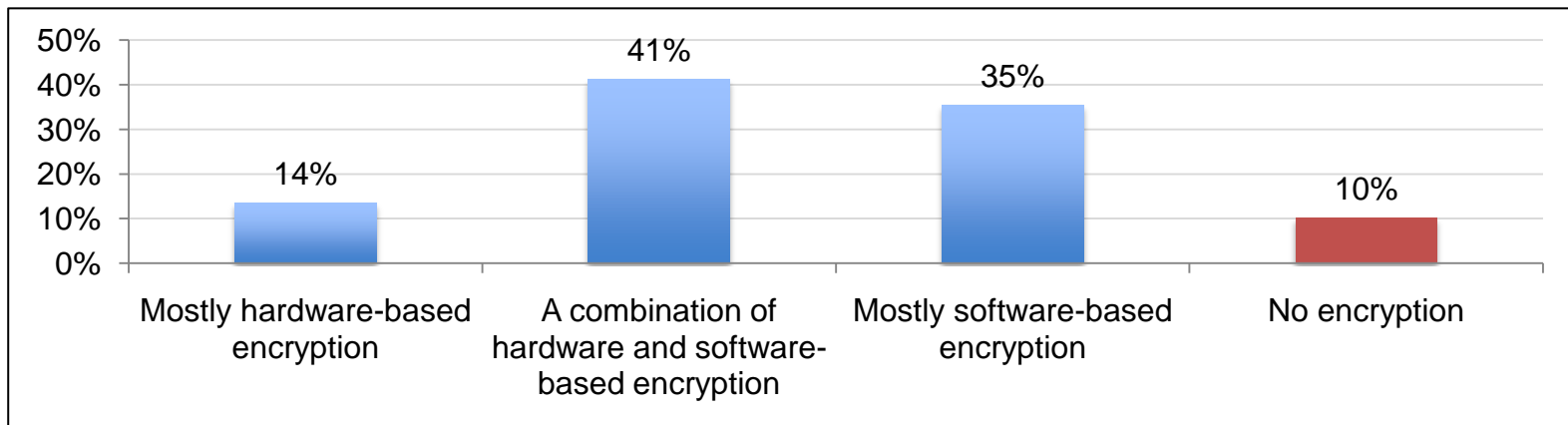


Screening questions

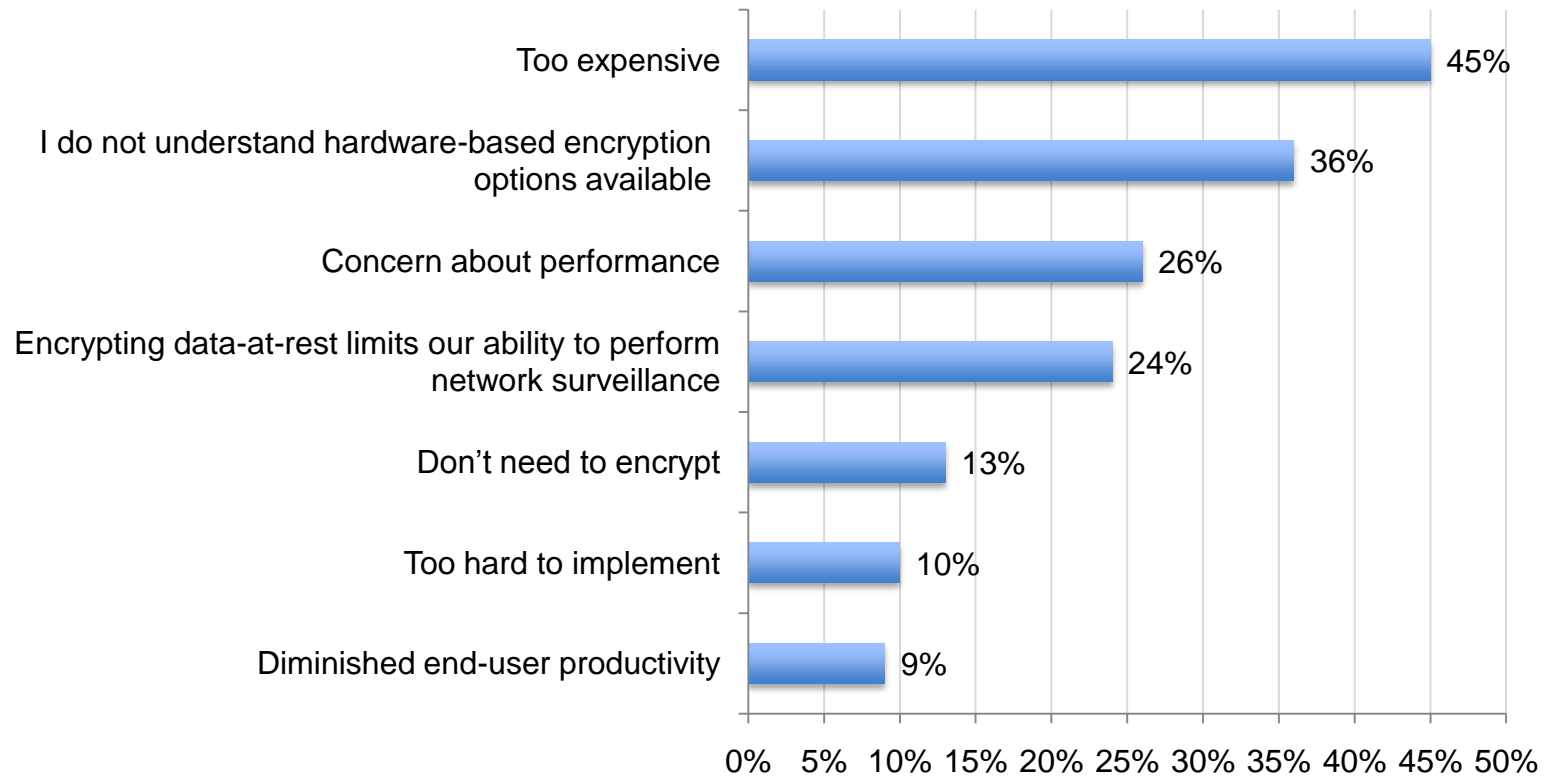
How familiar are you with self-encrypting (SED) drives?



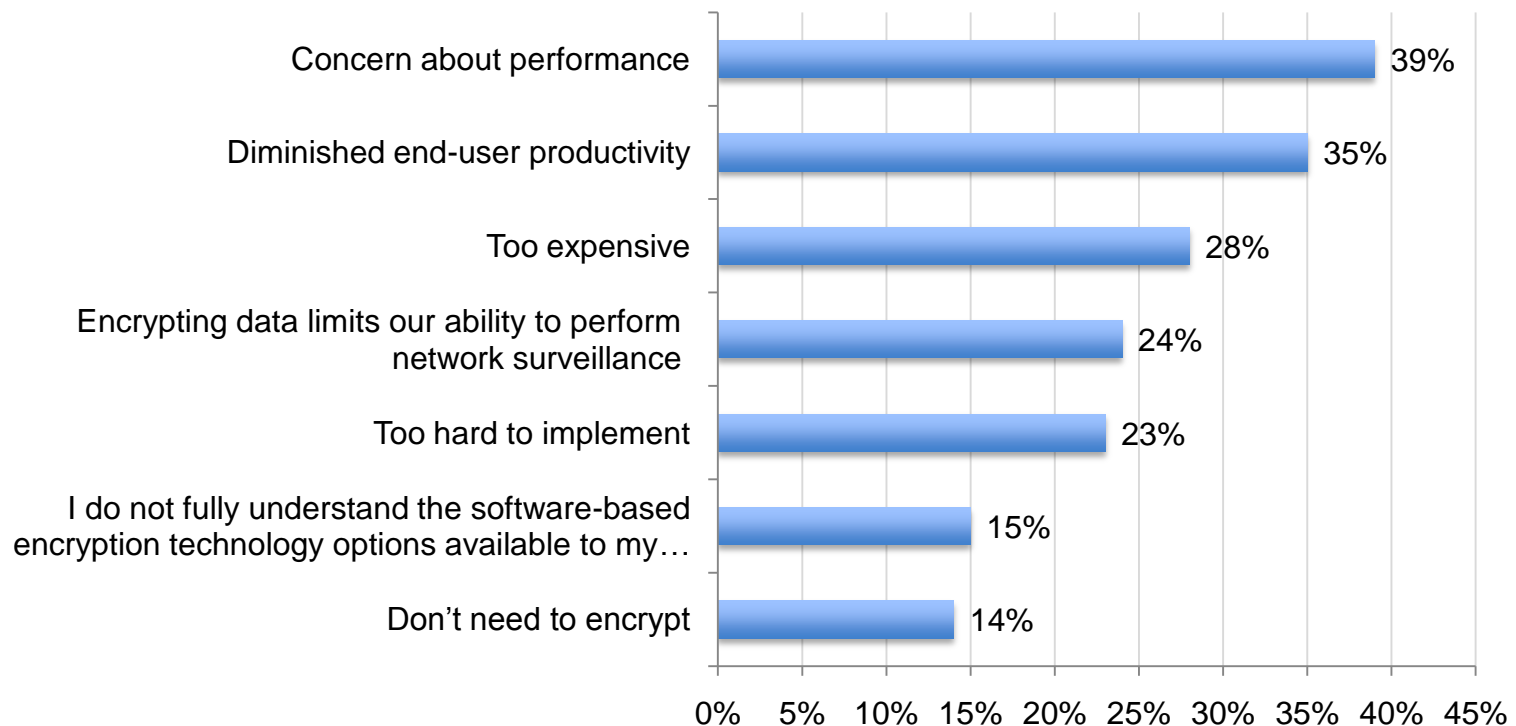
Does your organization use hardware or software-based encryption for protecting stored data on drives?



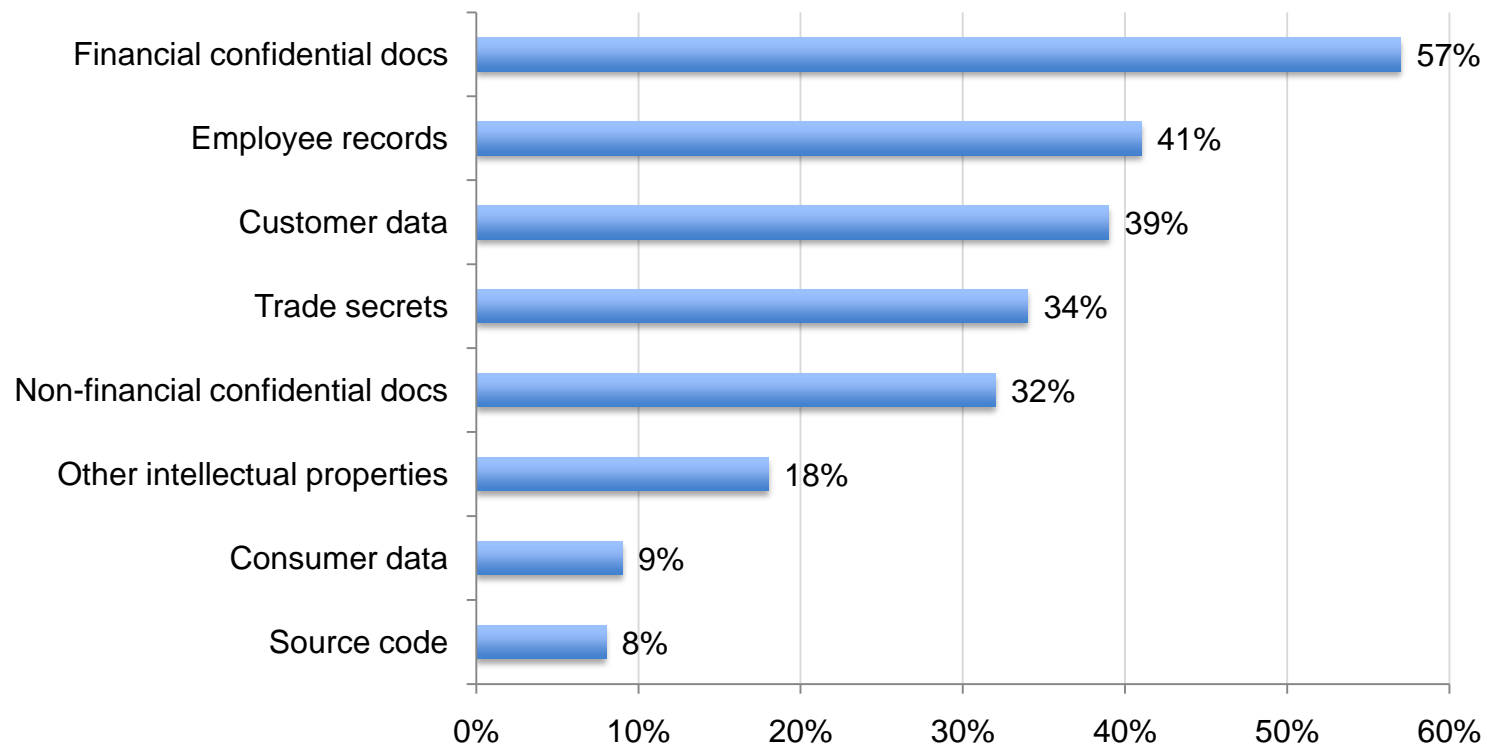
If your organization is not using hardware-based encryption, why not?



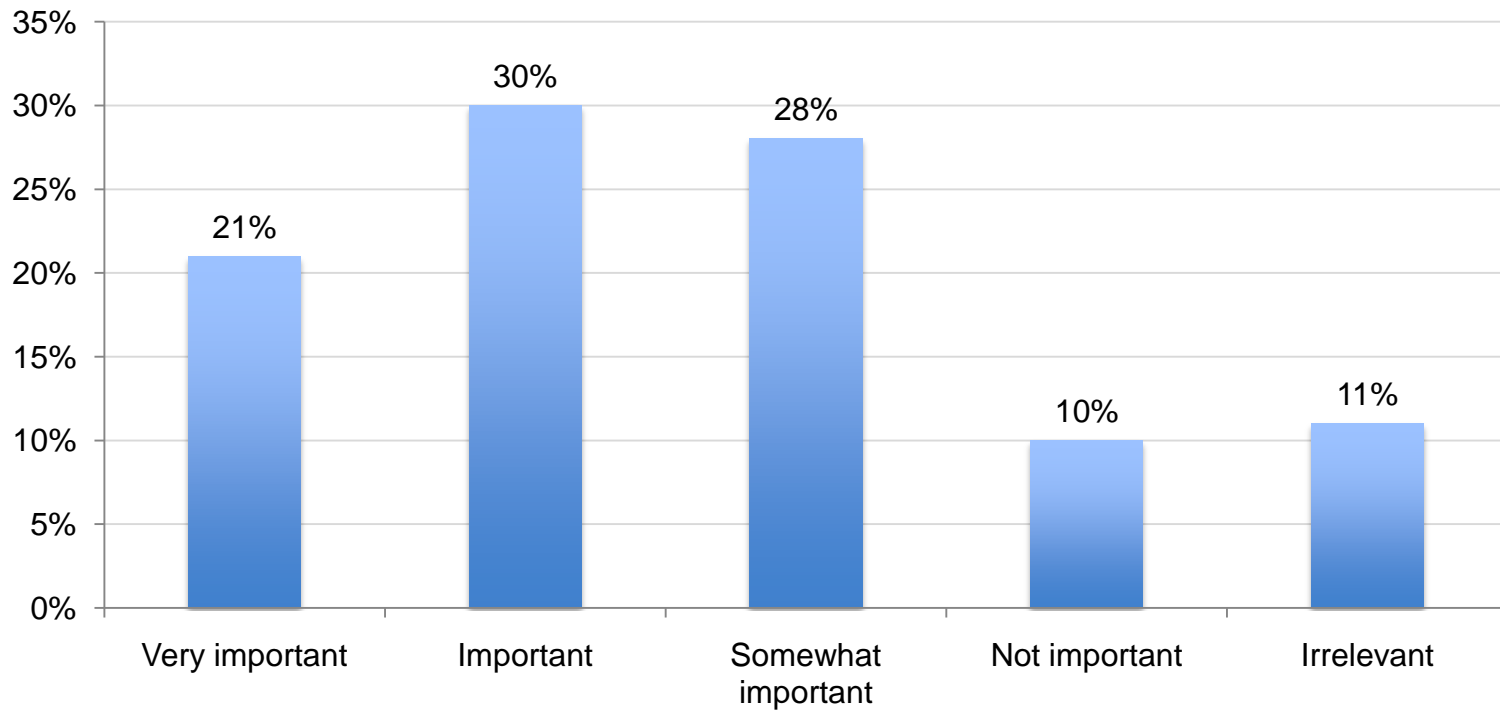
If your organization is not using software-based encryption, why not?



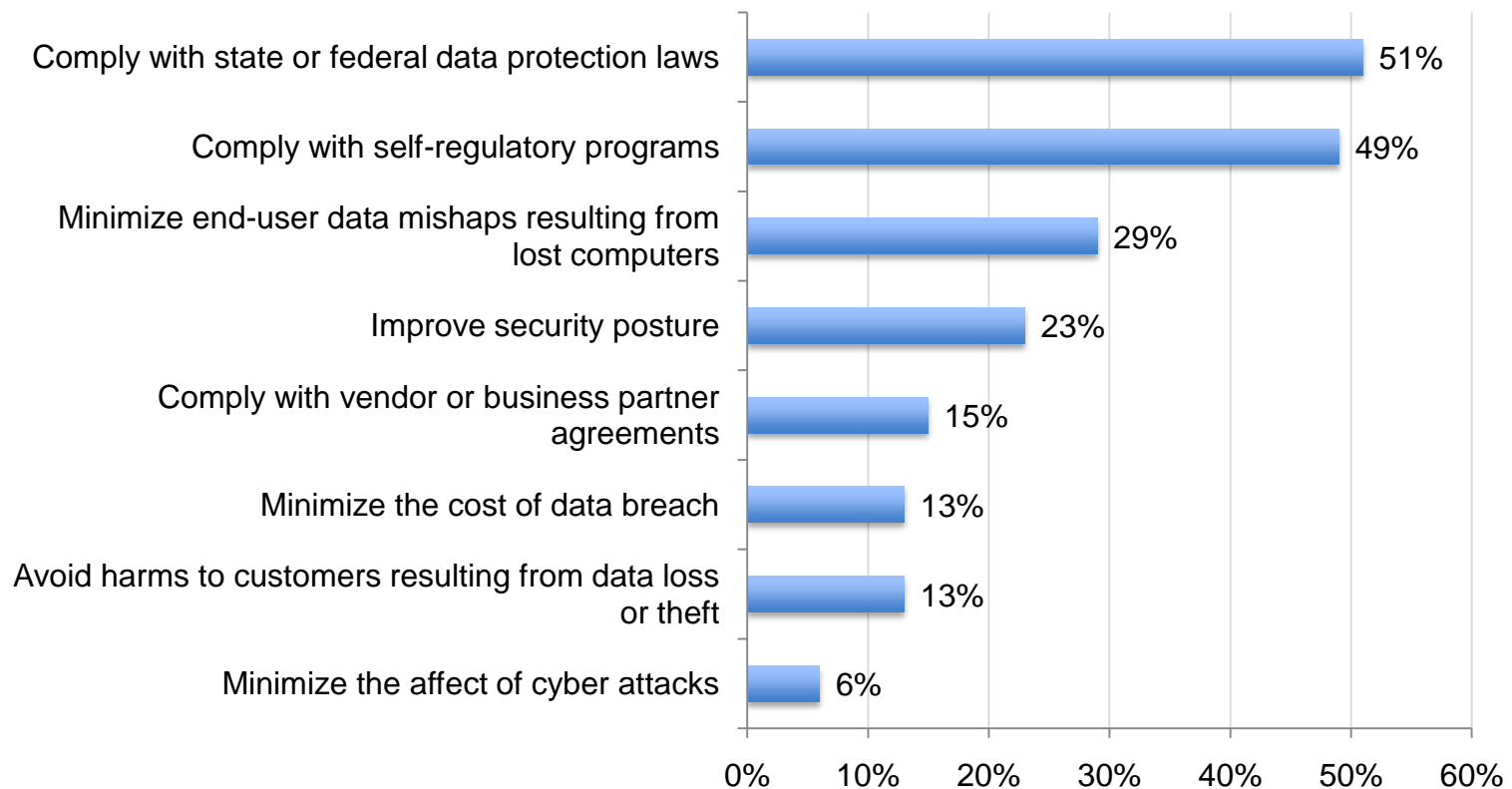
What types of stored data on drives are normally encrypted in your organization?



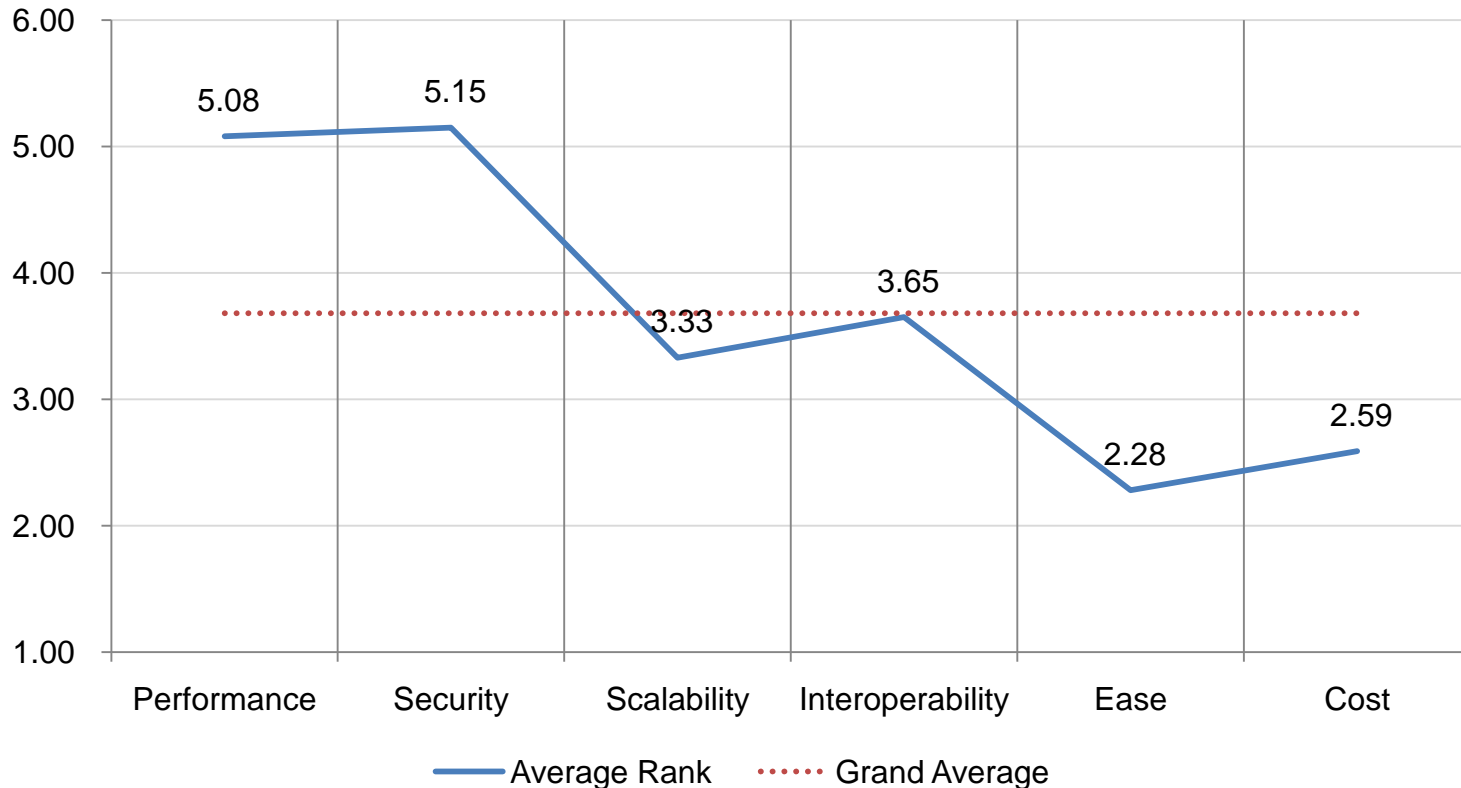
How important is compliance with high security standards such as FIPS 197 (AES) or FIPS 140 to your decision to select a drive encryption solutions?



Why does your organization encrypt data-at-rest? Top two choices

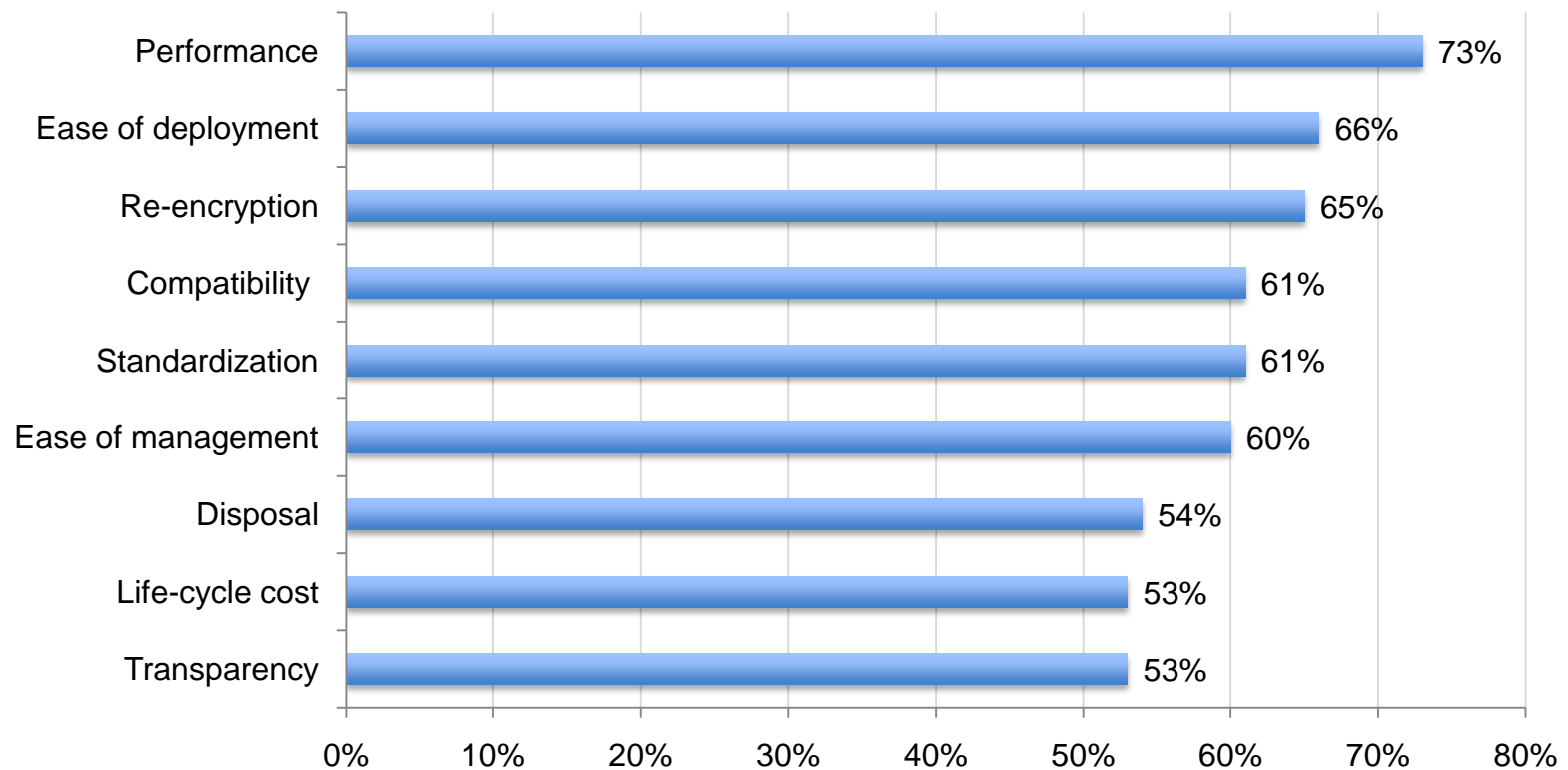


In evaluating encryption solutions for your organization, how important is each attribute listed below? From 6 = most important to 1 = least important.



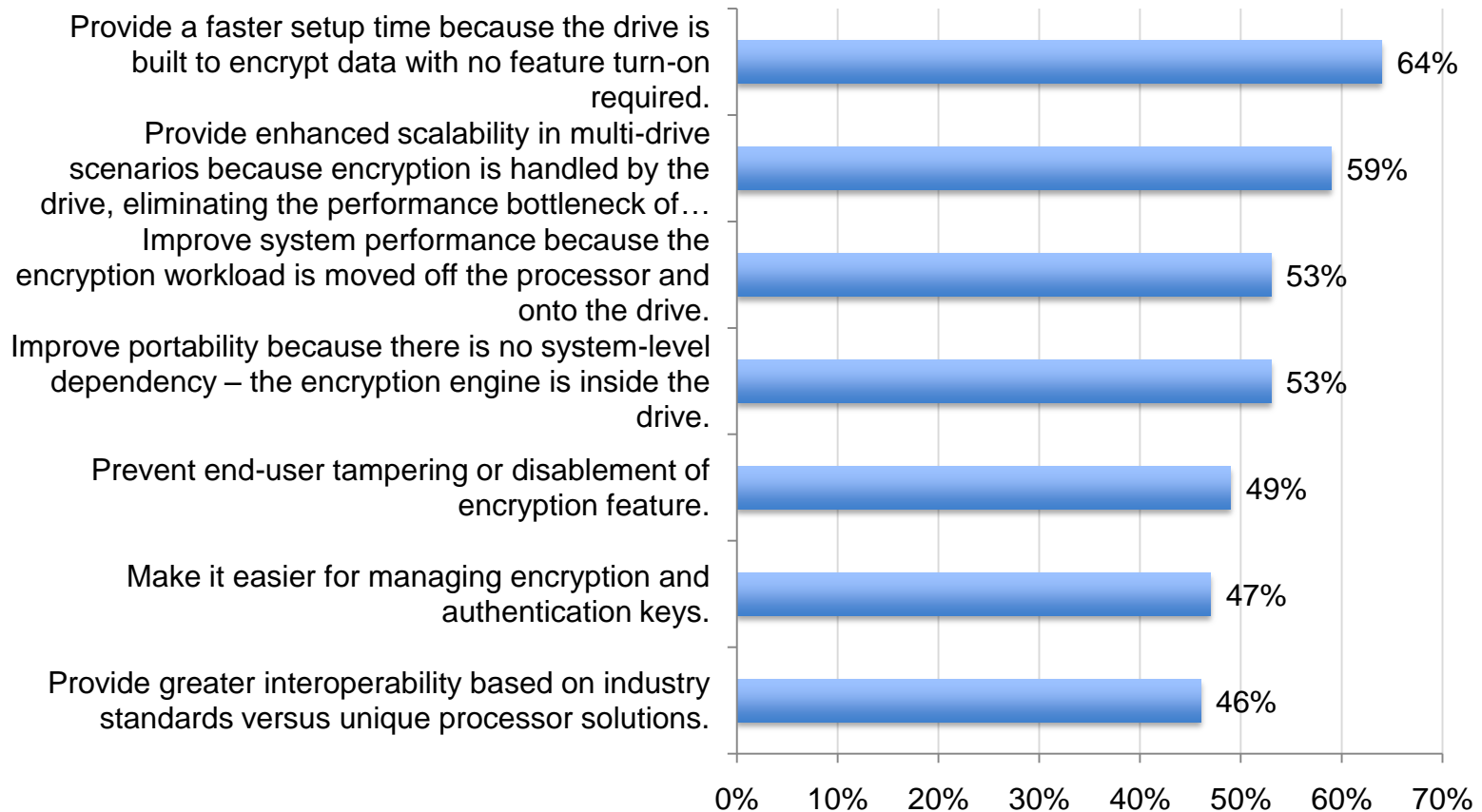
Please rate the importance of each one of the following nine drive encryption features

Each bar reflects the very important and importance response combined

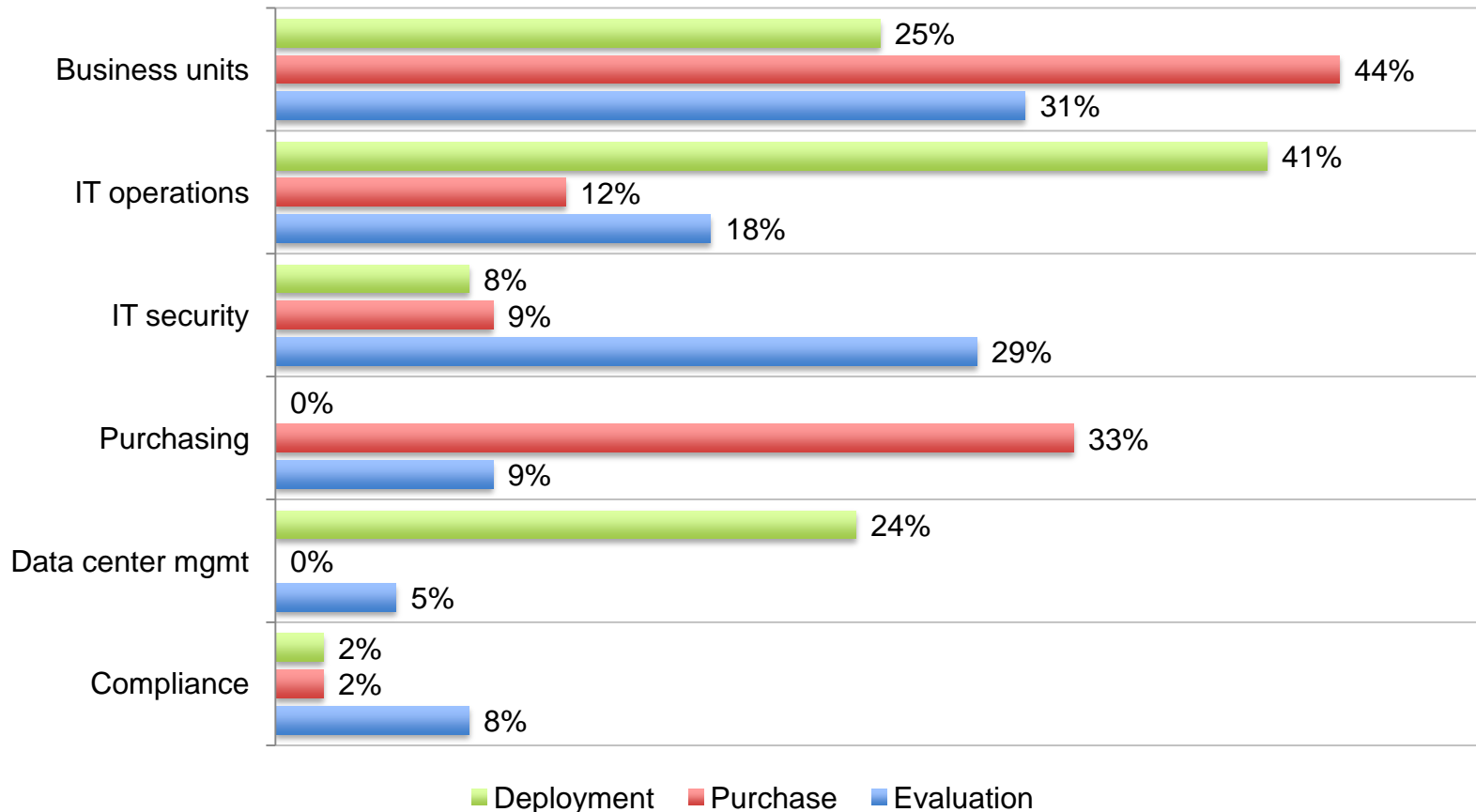


In comparison to software-based encrypted drives, SEDs do the following:

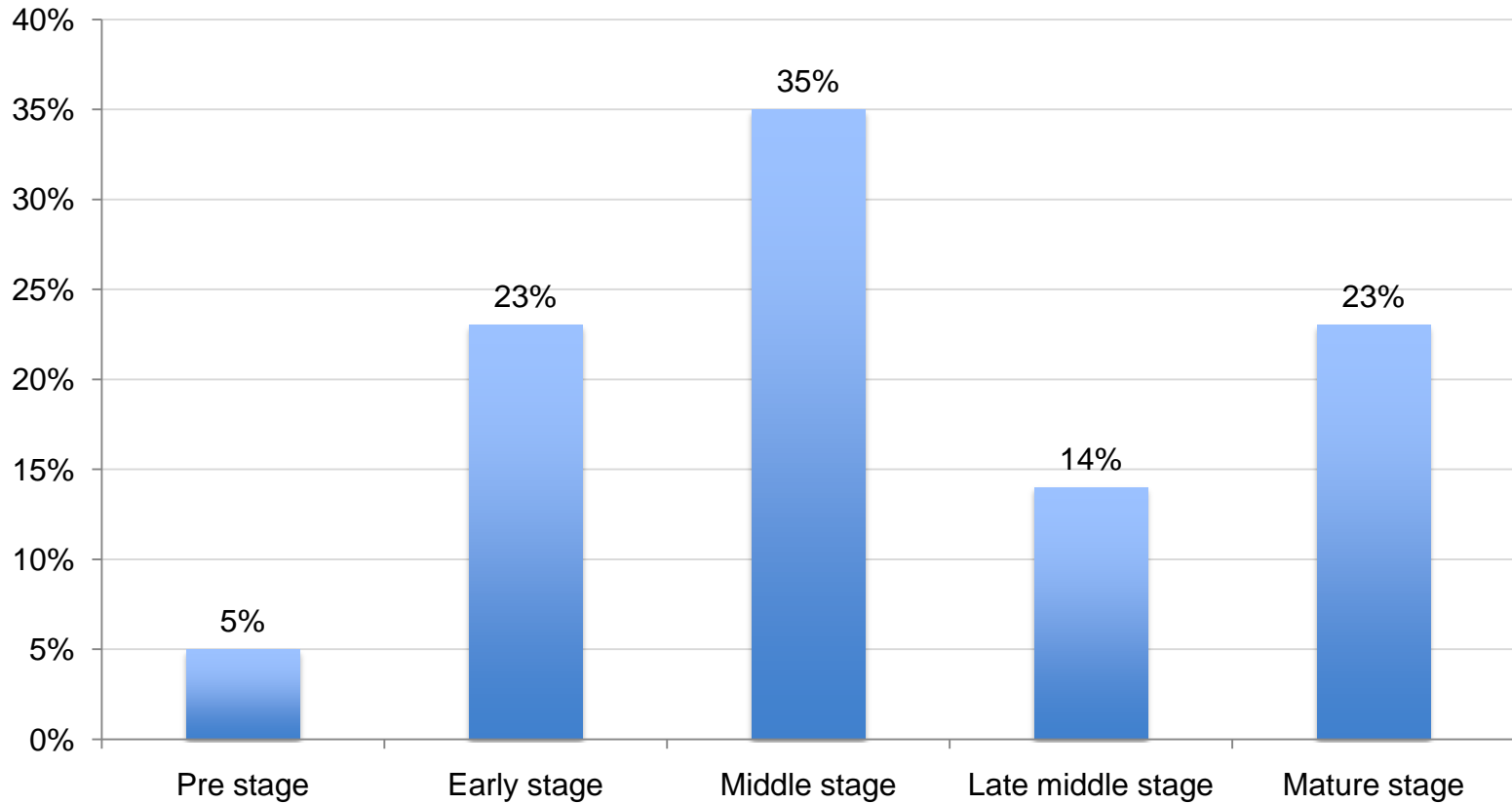
Each bar reflects the strongly agree and agree response combined



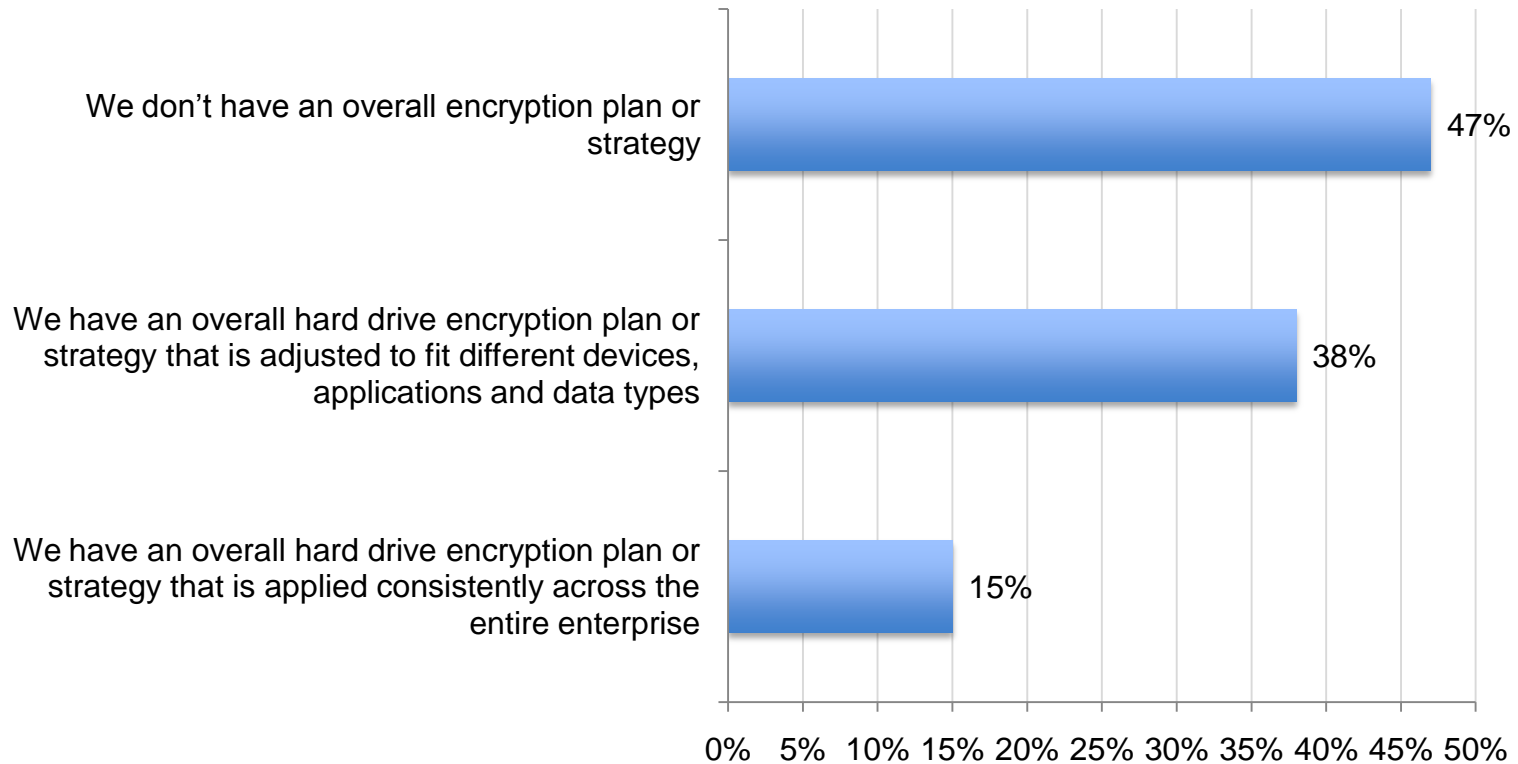
What departments or operating units within your organization are most responsible for: (1) evaluating, (2) purchasing or (3) deploying encryption solutions for drive storage devices



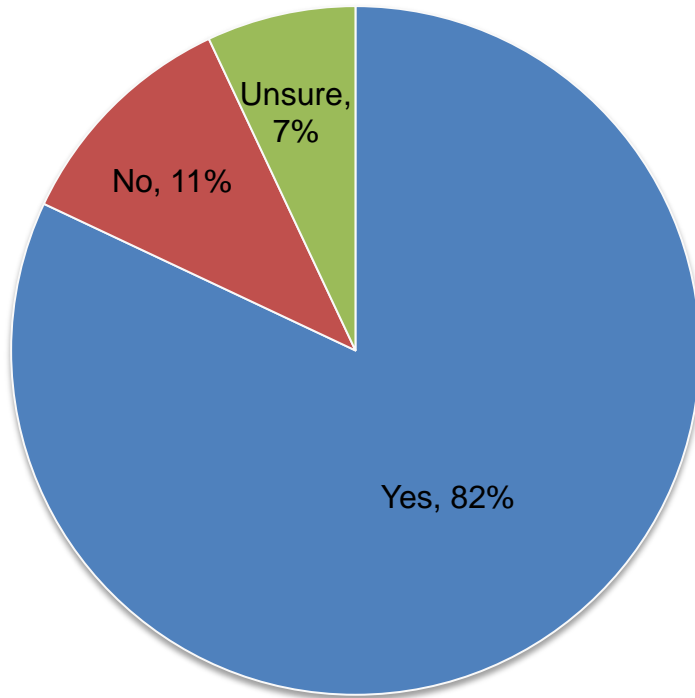
Please check the maturity stage of your company's information security and data protection program



Please check one statement that best describes your organization's approach to drive encryption implementation across the enterprise

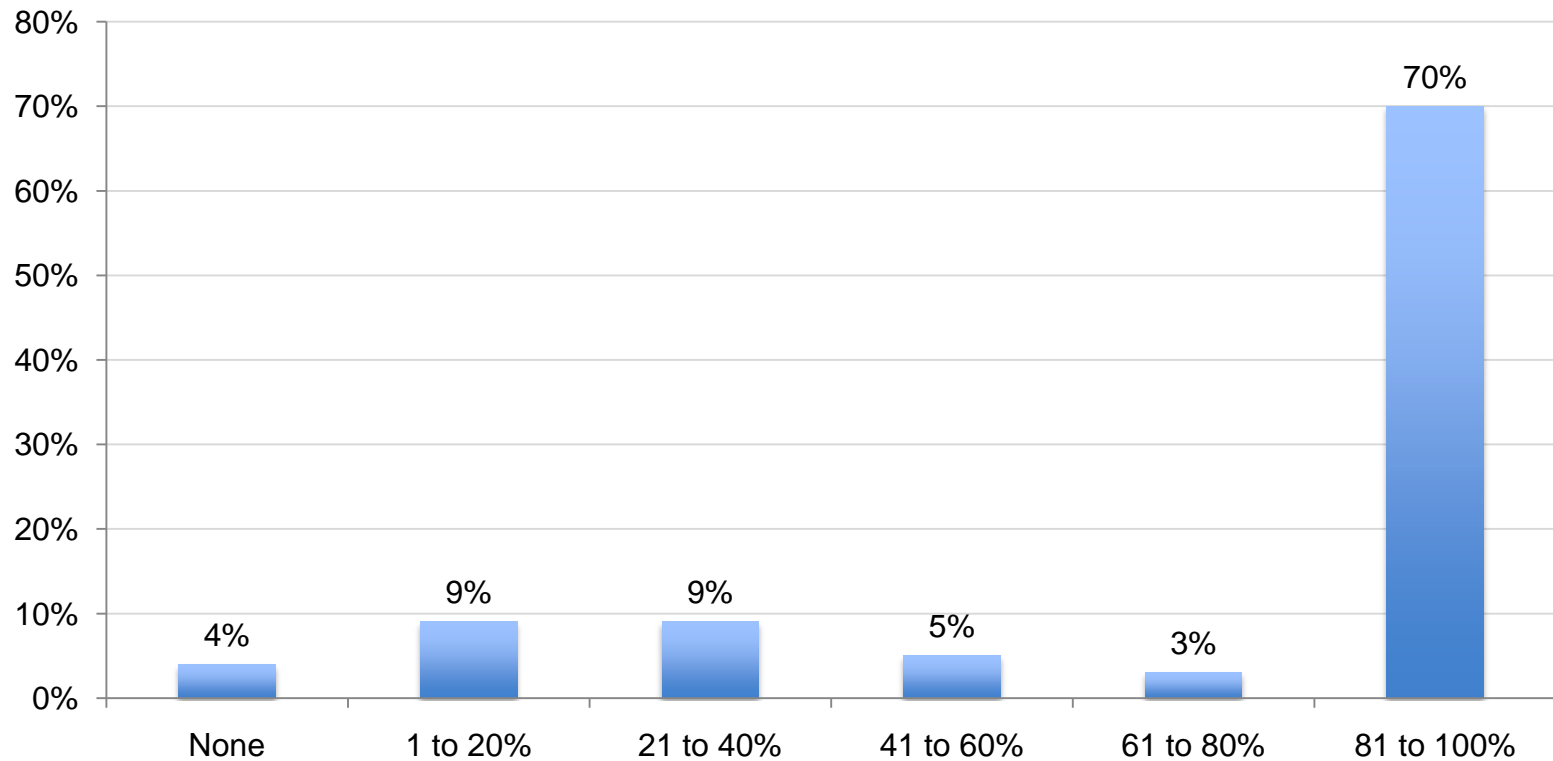


Did your organization experience one or more data breach incidents over the past 24 months?

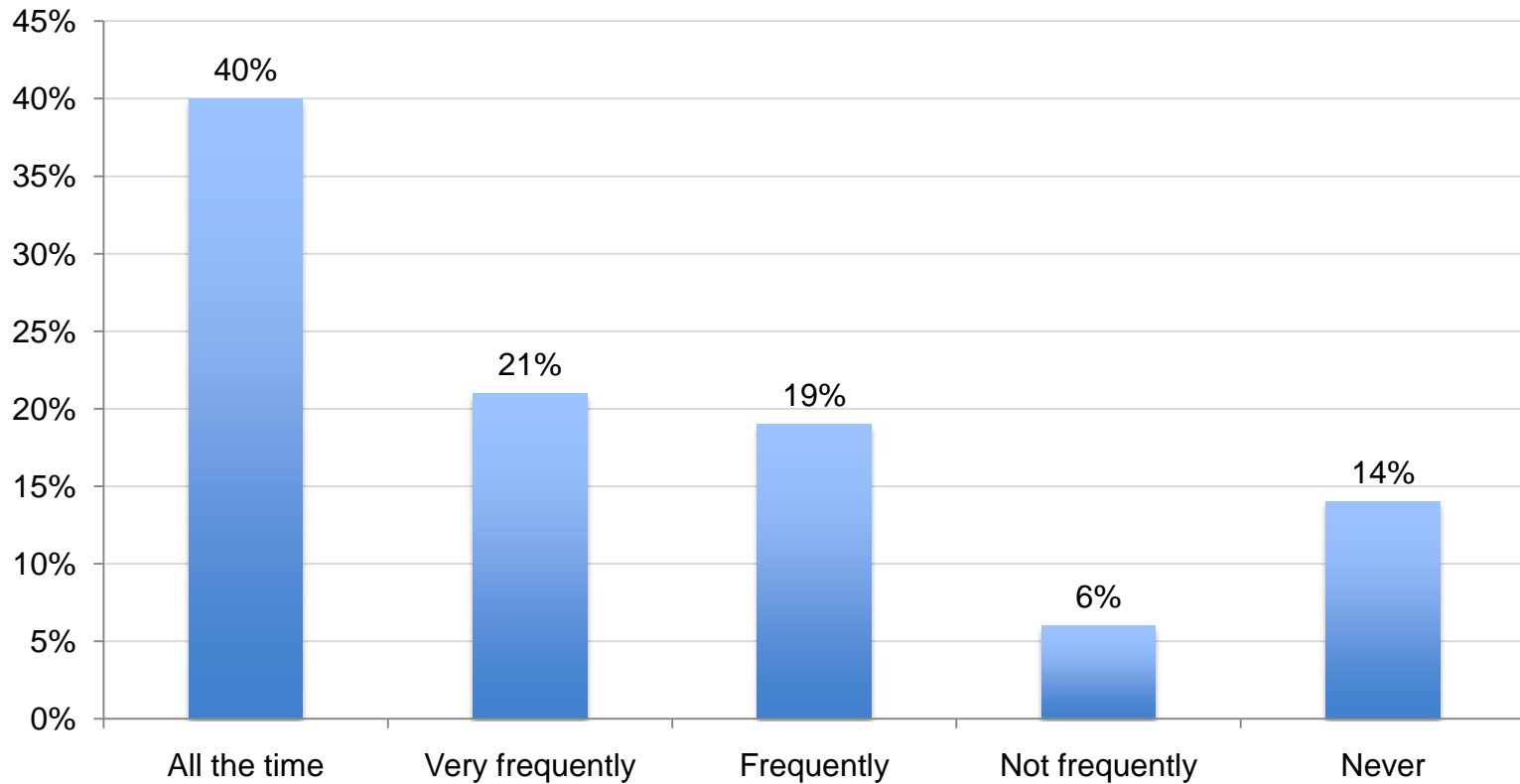


If yes, how many records were lost or stolen as a result of the above data breach incidents over the past 24 months?	Pct%
1 to 1,000	55%
1,000 to 5,000	23%
5,001 to 10,000	17%
10,001 to 50,000	2%
50,001 to 100,001	1%
100,001 to 500,000	1%
500,000 to 1,000,000	0%
More than 1,000,000	1%
Total	100%
Extrapolated average number of compromised records	15,875

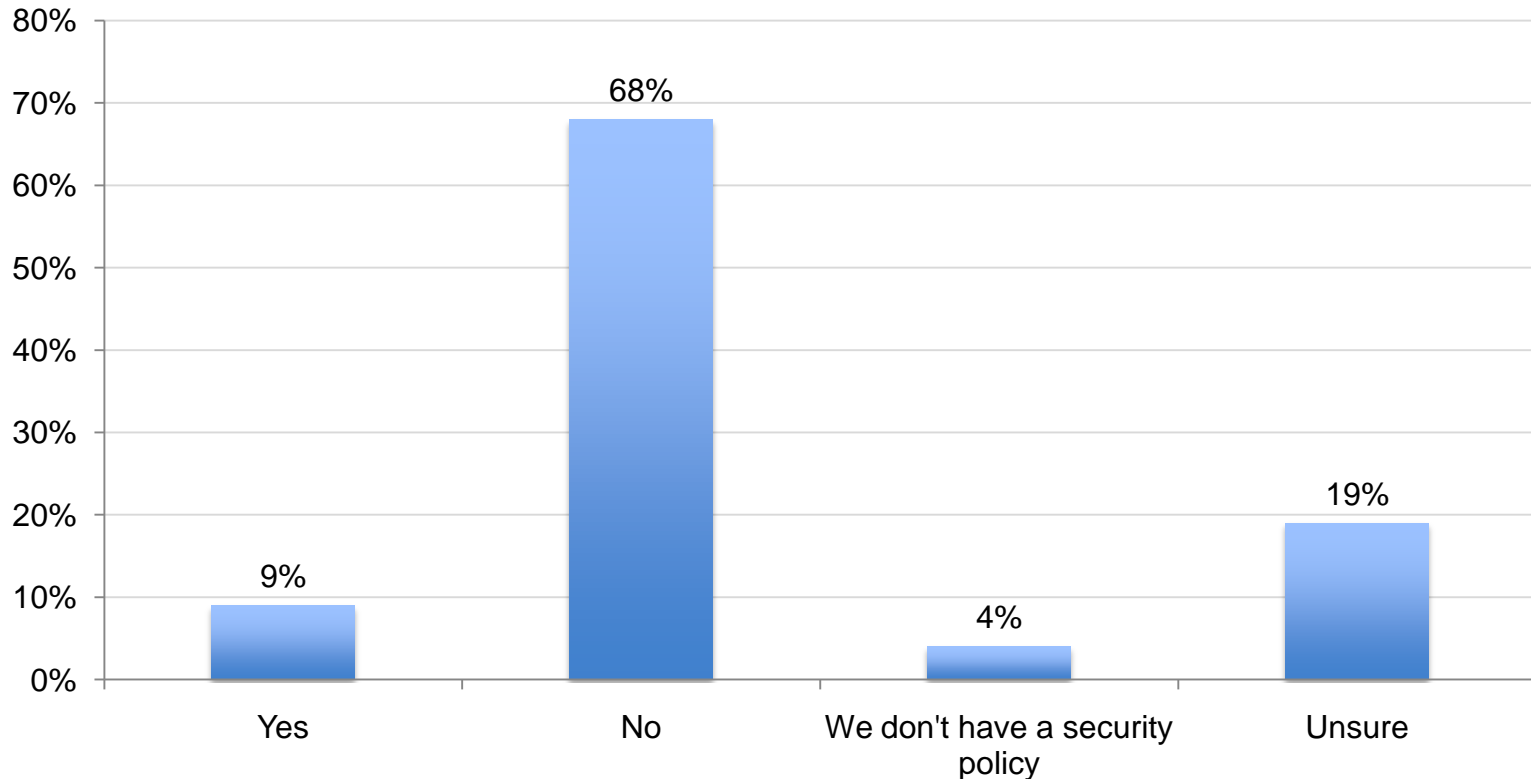
What percentage of these lost or stolen records would have been protected from abuse if they had been on self-encrypting drives?



Employees (end-users) turn-off or disengage their laptop's security protection without obtaining advance permission to do so

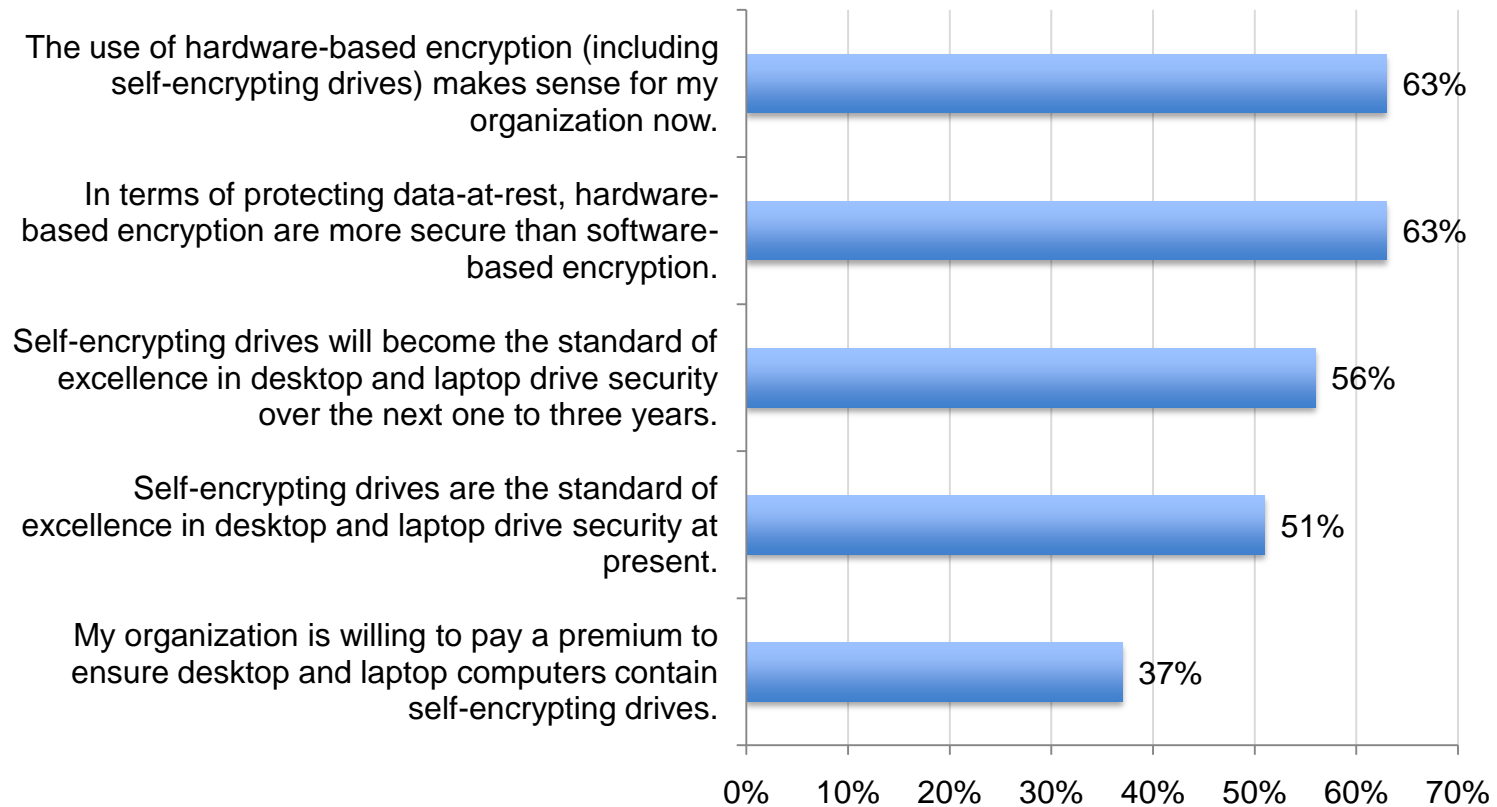


Does your organization's security policy allow employees (end-users) to turn-off or disengage their laptop's security protections including encryption?



Attributions about hardware-based encryption

Each bar reflects the strongly agree and agree response combined



Sample demographics

Check the Primary Person you or your IT security leader reports to within the organization.	Pct%
CEO/Executive Committee	1%
Chief Financial Officer	2%
General Counsel	2%
Chief Information Officer	56%
Compliance Officer	9%
Human Resources VP	2%
Head of information security (CISO)	15%
Head of security (CSO)	5%
Chief Risk Officer	6%
Other	2%
Total	100%

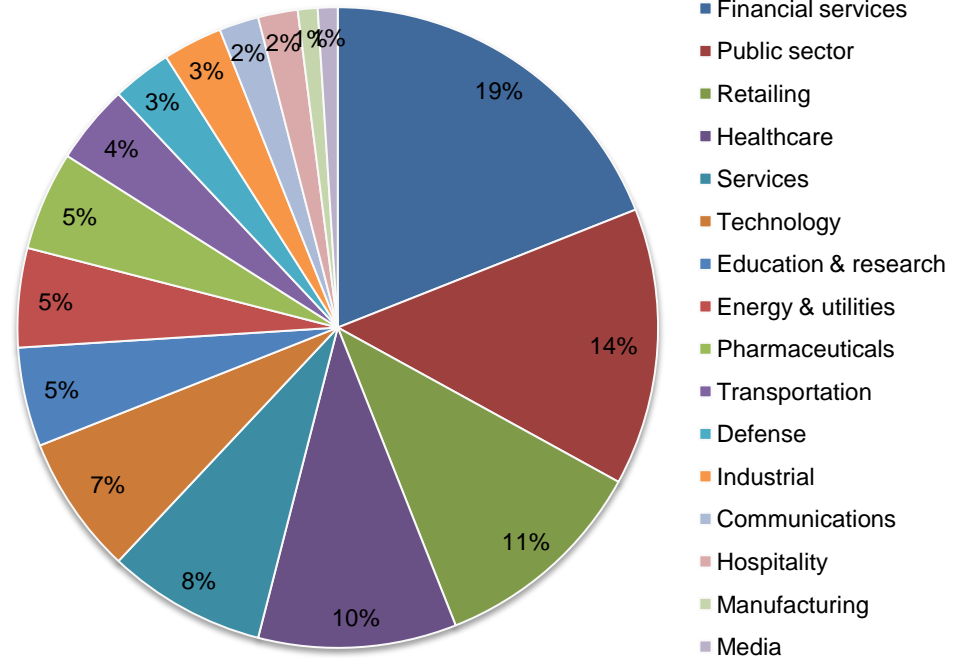
D4. Total years of relevant experience	Mean
Total years of IT or security experience	9.55
Total years in current position	4.51

Gender	Pct%
Female	28%
Male	72%
Total	100%

Sample demographics

Where are your employees located? (Check all that apply):	Pct%
United States	100%
Canada	63%
Europe	61%
Middle east	28%
Asia-Pacific	49%
Latin America (including Mexico)	50%
Total	351%

What is the worldwide headcount of your organization?	Pct%
Less than 500 people	9%
500 to 1,000 people	18%
1,001 to 5,000 people	23%
5,001 to 25,000 people	22%
25,001 to 75,000 people	20%
More than 75,000 people	8%
Total	100%





Questions?

Ponemon Institute

www.ponemon.org

Tel: 231.938.9900

Toll Free: 800.887.3118

Michigan HQ: 2308 US 31 N. Traverse City, MI 49686

research@ponemon.org

Trusted Computing Group

www.trustedcomputinggroup.org

Tel: 503.619.0562

3855 SW 153rd Drive Beaverton, OR 97006

admin@trustedcomputinggroup.org



Thank You for Attending

Additional Resources:

- Trusted Computing Group:
 - www.trustedcomputinggroup.org/solutions/data_protection
 - <http://www.trustedcomputinggroup.org/developers/storage>
- Ponemon Institute
 - www.ponemoninstitute.org

Live Webcast Archive to be available within 48 hours at:

http://www.trustedcomputinggroup.org/media_room/events/99

BACK-UP

Bio - Dr. Larry Ponemon

- **Dr. Larry Ponemon** is the Chairman and Founder of the Ponemon Institute, a research “think tank” dedicated to advancing privacy and data protection practices. Dr. Ponemon is considered a pioneer in privacy auditing and the Responsible Information Management or RIM framework.
- Ponemon Institute conducts independent research, educates leaders from the private and public sectors and verifies the privacy and data protection practices of organizations in a various industries. In addition to Institute activities, Dr. Ponemon is an adjunct professor for ethics and privacy at Carnegie Mellon University’s CIO Institute. He is a Fellow of the Center for Government Innovation of the Unisys Corporation